Matt Zagame

Dr. Haim Levkowitz

Mobile App Programming II

April 13, 2022

# Self-Sovereign Identity and The Internet

## Abstract

Self-sovereign identity is a concept that proposes to redefine digital identity on the Internet. Currently, the Internet does not handle digital identity in a way that is consistent with physical identity. This is primarily due to the platformization and centralization of the web. Self-sovereign identity changes this by allowing users to be in control of their own data through the use of distributed computing technology, i.e. blockchain. Topics covered in this paper include an introduction to the problem that self-sovereign identity solves, how digital identity will transform over time, a summary of the current defining principles of self-sovereign identity, as well as an analysis of the proposed architectural components. Each of the principles of a self-sovereign identity can be grouped into one of three categories which are, security, control, and portability. In terms of architectural design, four components are examined as they relate to blockchain technology; these are, identification, authentication, verifiable claims, and attribute storage. Altogether, self-sovereign identity creates a truly trustless and verifiable system of digital identity.

# Introduction

In the early days of the Internet, it was near impossible to verifiably prove anyone's physical identity. In fact, the Internet was not created with identity in mind, it was created so that machines could route information throughout networks without needing a third-party's authorization. However, given how quickly the Internet was adopted and commercialized, it didn't take long before websites began to require users to create accounts in order to use their services. Accessing an account would typically only require two user-generated credentials: a username and a password. Soon after, email became the primary means of verifying ownership of an account and helped to prevent the creation of spam accounts. Online identity has since experienced only slight improvements, such as platform-specific security and privacy options.

The problem with the Internet's current identity model is that it is fragmented across various platforms and services. In most cases, an email and password is required to create a unique online account. It is then the user's responsibility to keep track of this information while it must also be stored on a database for each and every platform, demonstrating inefficiencies for both the user and in data storage. More recently, there has also been a push towards the use of two-factor authentication (2FA) which is largely the result of security concerns regarding the current model. Given that a majority of Internet users either forget their login credentials, struggle with 2FA, or are more generally concerned about the security or privacy of their identities online, it is clear that a solution to these problems is apropos. Hence, the inception of self-sovereign identity.

Self-sovereign identity is a concept that has recently emerged as a product of the success of distributed computing systems. The aim of self-sovereign identity is to tackle the Internet's

inherent identity issue by allowing users to have identity relationships while being completely in control of their own data. In this sense, identity relationships are permissions to access a user's data that is granted to other individuals, websites or services. Allowing individuals control over their own identity means no third-party would be required for authorization or responsible for storing any user information. As for the implementation of self-sovereign identity, the general consensus is to leverage the decentralized nature of blockchain technology in order to support a network of identities. Distributed key management and encrypted peer-to-peer sharing of claims make this possible. In the next two sections, the necessary characteristics of a self-sovereign identity will be discussed, followed by an analysis of proposed architectures.

## Digital Identity on the Internet

As was originally put forward by Christopher Allen in his article, "The Path to Self-Sovereign Identity," the vision for self-sovereign identity is one that enables trust while preserving individual privacy (2016). Digital identity on the Internet currently requires a degree of trust in a third-party while using their services. For most, these third-parties are often common everyday names such as Google, Facebook, Twitter, and other online services that may not always disclose how user data is managed. As the presence of any platform grows larger on the web, users tend to become more reliant on their services which results in the centralization of user data. This model effectively brings about the antithesis of identity as it requires a third-party to maintain an identity for an individual. Which also leads into what is perhaps the largest concern for many in the digital age, data privacy. Since the platformization of the web, there have been countless incidents regarding breaches of user data, particularly with Facebook on the order of hundreds of millions of users' data being leaked (Bowman, 2021). An unfortunate reality that can largely be attributed to the fact that centralized servers make for easier targets for hackers.

Self-sovereign identity removes the barrier of third-party trust due to being completely decentralized. As digital identity solutions become less centralized over time, individual privacy concerns become less of an issue as well.

Alongside the excitement surrounding blockchain and distributed ledger technology in recent years, focus on digital self-sovereign identity solutions has slowly but surely begun to take place. Allen projects digital identity will develop in four phases, starting from centralized, to federated, to user-centric, to fully self-sovereign (2016). As of today, a majority of the Internet still operates on a centralized identity system such that a single authority or hierarchy has control over user data. Hierarchical systems in which smaller amounts of administrative control are delegated to subsidiaries are also ultimately centralized around a single entity. For instance, most social media platforms reserve the right to remove user profiles, erasing their identity from the platform (Sovrin, 2021). A second, more modern approach is the federated system which enables the use of a single account across numerous websites. One common example of this is when websites offer Google Sign-In as an option to login. However the root problem is still the same—it is still a centralized identity. The shift to a user-centric identity requires a user to have more control over his or her own identity and the decentralization of trust (Allen, 2016). One of the original methods deemed to be user-centric, OAuth, is now often associated with 2FA. The general blueprint for these systems is to work independently of any one provider and to require the user's consent before accessing his or her data. Yet these systems may also be insufficient if the registering entity decides to erase the user's data or the requested data is leaked (Sovrin, 2021). To create a truly self-sovereign system of identity, it needs to be governed solely by the user themselves. In other words, the greatest challenge of the Internet; allowing users to have an identity that is inherently theirs.

## Principles of Self-Sovereign Identity

In order to solve the Internet's identity problem, several principles must be taken into account. The principles that Christopher Allen established for a self-sovereign identity can be arranged into three main categories: security, control, and portability (Sovrin, 2021). Security should be prioritized since identity information is sensitive to the user. This can be done via decentralized selective-disclosure algorithms that only access required information while keeping everything else private. In addition, a user's identity should persist for as long as is desired. In this regard, blockchain's cryptographic and ledger-like properties make for a secure store of identity information. Control, as has been previously stated, must remain completely with the user. This means a few things. For starters, identities must exist independently of the Internet (Allen, 2016). This helps bridge the gap between physical and digital identity, which also ties into the aspect of identity persisting with the user themselves. Most importantly, a user must be able to decide what is shared and with whom at his or her own discretion. Identity is a user's right and any request for information should require user consent. Portability, being the third category, mandates that a digital identity behaves just like a physical identity such that it can be used anywhere at any time. The decentralized technology used to support self-sovereign identity should be both interoperable and transparent. Successfully building a secure and trustless identity layer for the Internet means that the algorithms upon which it is built should be open-source just like the Internet. Putting it all together, these fundamental principles will serve well as a guide for the future of digital identity.

## Analysis

At its core, self-sovereign identity is a decentralized identity management system. Any functional decentralized identity system will have at least a few moving parts. Following an

exemplary survey conducted by Alexander Mühle et al., this analysis will focus on four key components of a self-sovereign identity which are identification, authentication, verifiable claims, and attribute storage (2018). The first two components, identification and authentication, are handled by the blockchain which serves as a distributed record of information; making it ideal for managing a network of identities. The latter two components, verifiable claims and attribute storage, are directly controlled by the user. Authentication is a relatively simple process that involves four entities, a claim issuer, a relying party, the blockchain, and the user themselves. As a requirement, the user must have ownership of a unique identifier, which in this case is a cryptographic key. A public authentication method along with the user's cryptographic key is then used to register a claim on the blockchain. It is worth noting that all claims and attestations relating to the user are stored and managed privately by the user. Neither the claim issuer nor the relying party needs to store information about the user for this system to work. Assuming the relying party has established trust with the claim issuer, the identity may then be verified by the relying party. On the whole, this approach to an architecture for self-sovereign identity properly satisfies each of the defining principles, offering control, security and portability.

## Conclusion

The Internet has de facto been built on a model that is absent of identity. Currently, a user must create an identity that is tied to a specific platform or service(s). Authentication then requires remembrance of platform-specific credentials which already makes the whole process much less intrinsic for the average user. In addition, the current model requires a degree of trust in a third-party to keep sensitive information secure. As increasingly many people are forced to live out their daily lives on various platforms online, the idea of self-sovereign identity has become

ever more appealing. As for the future of digital identity, the recent rise in adoption of distributed computing systems is well-positioned to be the catalyst that leads to a better solution. In fact, prominent organizations such as the Sovrin Foundation and the W3C have already begun to get involved with decentralized identity solutions. In other words, self-sovereign identity could soon play an important role in online activities.

## References


Allen, Christopher. “Life with Alacrity.” The Path to Self-Sovereign Identity, 25 Apr. 2016, http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

Bowman, Emma. “After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users.” NPR, NPR, 10 Apr. 2021, https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users.

“Decentralized Identifiers (Dids) v1.0.” W3C, https://www.w3.org/TR/did-core/#abstract.

“Inevitable Rise of Self-Sovereign Identity.” Sovrin, 1 Nov. 2021, https://sovrin.org/library/inevitable-rise-of-self-sovereign-identity/.

Mühle, Alexander, et al. “A Survey on Essential Components of a Self-Sovereign Identity.” Computer Science Review, Elsevier, 25 Oct. 2018, https://www.sciencedirect.com/science/article/pii/S1574013718301217.